REMARKS

This amendment is submitted in response to the Examiner's Action dated December 15, 2004. Applicants have amended the specification to overcome objections thereto and objections to the drawings. Applicants have also amended the claims to clarify key features of the invention and overcome the claim rejections. No new matter has been added, and the amendments place the claims in better condition for allowance. Applicants respectfully request entry of the amendments to the claims. The discussion/arguments provided below reference the claims in their amended form.

IN THE SPECIFICATION

In the present Office Action, the disclosure is objected to because of several listed informalities. Applicants have reviewed the disclosure and provided corrections to most of the informalities listed. Applicants assume the last of these objections is a reference to page 8, line 13, and not page 5, line 13. The corrections are presented in the above section titled "Amendments in the Specification." Applicants respectfully request entry of the amendments to the specification and removal of the objections thereto. Finally, Applicants address the objection related to the reference to Figures 3A-3D, in the section below.

IN THE DRAWINGS

In the present Office Action, the drawings are objected to because of informalities. With respect to the first objection, Applicants have amended the text of the specification to remove the reference numeral (200). It appears that the second objection is directed at informal drawings filed with the application on April 6, 2001. However, Applicants filed new formal drawings on July 25, 2001 that were received in the USPTO on July 30, 2001. These drawings include the labels Figures 3A - 3D, and renders the objection moot. Applicants submit herewith a duplicate copy of the filed formal drawings, which overcome the objections.

CLAIM REJECTIONS UNDER 35 U.S.C. § 103

In section 5 of the present Office Action, Claims 1-4, 9-12 and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Bellovin* (U.S. Patent No. 5,241,599) in view of *Liao, et al.* (U.S. Patent No. 6,263,437). In section 12 of the present Office Action, Claims 5-7, 13-15 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Bellovin* in view of *Liao, et al.* and further in view of *Ramasubramani, et al.*. In section 14 of the present Office Action, Claims 8, 16 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Bellovin* in view of *Liao, et al.* further in view of *Ramasubramani, et al.* further in view of I/O Concepts Inc., Title Console Consolidation System Overview (*I/O Concepts)*.

Finally, in section 7 of the present Office Action, Claims 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Liao, et al.* in view of *Ramasubramani, et al.* (U.S. Patent No. 6,233,577).

Applicants have amended the above referenced claims to more clearly recite the novel features of Applicants' invention. As described within the specification, Applicants' invention provides a dual authentication process for accessing a network-based computer system from a network-connected console device. The dual authentication involves a first EKE sequence by which the console device itself is authenticated for accessing the network-based computer system. The authentication is completed using a shared secret generated during a previous session (or during set up of the console device), which shared secret is generated using a default device ID and default secret. Once the console device is authenticated, the operator/user ID and password are then authenticated via a second EKE sequence involving the console device and the network-based computer system.

During the second EKE sequence, the shared secret of the first EKE sequence is utilized to encrypt and decrypt the user ID and password being passed between the two devices. Also, following the authentication of the user ID and password, the secret generated by the second EKE sequence is utilized to encrypt and decrypt session data transmitted during the session.

Applicants' amended claims now more clearly recite the above features. For example, Claim 1 now recites:

> *initiating a **first EKE sequence** between a console device and a network-accessible system **to authenticate the console device** ...; ... initiating **a second EKE sequence** between the console device and the network-accessible system **to authenticate a userID and password** of the user of the console device; and **preventing access to the network-accessible system when either the first EKE sequence or the second EKE sequence fails to authenticate**, wherein a dual authentication procedure is implemented before any access is permitted by a user to the network-accessible system.*
> (emphases added)

Other features recited by various dependent claims include:

"**generating the device shared secret** via an initial EKE sequence **utilizing a default device identifier and associated default shared secret** ..." (Claim 2);

"**encrypting and decrypting** subsequent session data flowing between said console device and said network-accessible system **utilizing** a value selected from among **a second secret** generated by the second EKE sequence **or a hash** of said second secret" (Claim 4); and

"...an embedded smart chip, storing the copy of the device shared secret within the embedded smart chip ..." (Claim 8).

The above references do not suggest, neither independently nor in combination with each other, any of the above features of Applicants' claimed invention. For example, *Bellovin* does not teach or suggest a dual authentication process. *Bellovin* describes a method for creating a **single** authenticated shared secret key using a back and forth challenge between two systems (Abstract; Fig. 1 and 2). Examiner correctly states that *Bellovin* does not teach storing the device shared secret or generating the device-specific shared secret utilizing a default device identifier.

Liao also does not teach the use of a dual authentication process. More specifically, *Liao* does not teach or suggest generating a device-specific shared secret using the device identifier. The section of *Liao* referenced by Examiner, col. 11, lines 56-59, states: "*The client module then sends a key request signal 406 to the server device 370. The key request signal 406 comprises the device ID 316 of the client device 302 and the generated client public value.*" Then, as is

stated within the Abstract, "*[e]ach side generates its own secret key from a self-generated private value along with the received counterpart's public value...*" This makes it very clear that *Liao* generates the secret key from a value other than the device identifier.

Examiner attempts to piece together *Ramasubramani*'s process, which includes mention of a username and password with the above references. However, nowhere in *Ramasubramani* or in any of the other references is there any support for an obviousness rejection of Applicants' dual authentication process, which includes an authentication of a user ID and password. Each reference clearly lays out a single method for authenticating either a device or a user, respectively, with no overlap or combination of methods provided in (or suggested by) any one of the references. Notably also, *Ramasubramani* does not actually require an authentication of a user ID and password to gain access to the system.

Ramasubramani presents is a description of a verification process involving the device ID itself, but *Ramasubramani* makes no reference to r suggestion of a secret key generated using the device ID. At col. 9, line 18-24, *Ramasubramani* states "*the username and password are not required information for the mobile device 302 to access the account 324, rather the user is given a permission to administrate .:. new username and password...*" This directly contradicts Applicants specific requirement for an authentication of the user ID and password before access is permitted to the system from the console.

Finally, Applicants note that Examiner relies on *I/O Concepts* without providing any indication of the exact date of publication of the article. While the article has a copyright notice dated 2000, Applicant is unable to ascertain when in 2000 the article was published. This information is necessary to confirm whether the article was published prior to Applicants' date of conception (for 1.131 Affidavit purposes), assuming the article was published at the end of 2000.

Given the above reasons, it is clear that the combinations of references do not suggest key features of Applicants' invention. One skilled in the art would not find Applicants' invention unpatentable over the combinations of references. The above claims are therefore allowable.

CONCLUSION

Applicants have diligently responded to the Office Action by amending the specification to overcome objections to both the specification and drawings. Applicants have also amended the claims to clarify features therein and overcome the § 103 rejections. The amendments and supporting arguments overcome the § 103 rejections, and Applicants, therefore, respectfully request issuance of a Notice of Allowance for all claims now pending.

Applicants further request the Examiner contact the undersigned attorney of record at 512.343.6116 if such would further or expedite the prosecution of the present Application.

Respectfully submitted,

James E. Boice
Reg. No. 44,545
Dillon & Yudell LLP
8911 North Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512.343.6116

ATTORNEY FOR APPLICANT(S)